

Atty. Docket No. 389522

### **REMARKS/ARGUMENTS**

The amendments and remarks hereto attend to all outstanding issues in the pending Office Action of 23 Oct. 2006. Claims 1-16 remain pending in this application (hereinafter, the "402 Application), with claim 15 amended for clarity. Subtitled sections presented herein below correspond with the order of issues presented in the aforementioned Office Action.

#### **1-5. Summary, Continued Examination and Response to Arguments**

We thank the Examiner for his concise summary of the status of the '402 Application. We note the withdrawal of finality of the previous Office Action, entry of Applicant's 16 Aug. 2006 submission, and the Examiner's consideration of the remarks presented therein.

#### **6. Claim Rejections – 35 U.S.C. § 112**

Claims 1-16 stand rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. In particular, the Examiner contends that the terms "unintelligible" and "useless," found in claims 1 and 15, are relative and indefinite. We respectfully disagree and traverse the rejection.

First, we respectfully direct the Examiner to MPEP 2173.05(b), which discusses relative claim terminology. Nowhere are the words "unintelligible" or "useless" mentioned. Both terms have recognized meanings and are understood not only by those of skill in the art, but also by the general public. For example, the Random House Unabridged Dictionary defines *unintelligible* as "not intelligible; not capable of being understood." *Dictionary.com Unabridged* (v 1.1), Random House, Inc., 1/18/07, <http://dictionary.reference.com/browse/unintelligible>. The same dictionary defines *useless* as "of no use; not serving the purpose or any purpose; unavailing or futile" or "without useful qualities; of no practical good." *Dictionary.com Unabridged* (v 1.1). Random House, Inc., 1/18/07, <http://dictionary.reference.com/browse/useless>. "Unintelligible" and "useless" are likewise understood within the arts of computer science, cryptography and within the patent literature in general.

Turning first to *unintelligible*, we note that the very practice of data encryption is defined as "the process of disguising information as "ciphertext," or data *unintelligible* to an unauthorized person. *Encyclopædia Britannica*, 2007, Encyclopædia Online, 1/18/07, <http://www.britannica.com/eb/article-9002217>, emphasis added. See also "data encryption" *The*

*Atty. Docket No. 389522*

*Columbia Encyclopedia*, Sixth Ed., 2006, at <http://www.encyclopedia.com/doc/1E1-dataencr.html>.

In another example, cryptography is defined as the "science of information security", which is achieved "by processing data (generally referred to as plaintext) into *unintelligible* form (ciphertext), reversibly, without data loss...The important concept to understand is that crypto is the application of mathematical algorithms to convert text into a form that is *unintelligible* to unauthorized viewers." Granger, Sarah, "Unlocking the Secrets of Crypto: Cryptography, Encryption, and Cryptology Explained," SecurityFocus at <http://www.securityfocus.com/infocus/1617>, emphasis added.

Further evidence that "undecipherable" is understood by those skilled in the art (indeed, by those in many arts) may be found at the USPTO Patent Search Page. A quick search on the USPTO patent search page revealed 79 issued patents with the word "unintelligible" in the claims. This includes 30 issued patents within U.S. Class 713, under which the '402 Application is categorized, and 13 issued patents within U.S. Class 380, under which the '402 Application has also been categorized. The word "unintelligible" appears in the abstract or specification of 195 patents within class 713, and in the abstract or specification of 431 patents with in class 380. See Appendix A, which includes the first page results of each search.

The meaning of *useless* is also well understood, both in general, as shown above, and by those skilled in the art. See Appendix B for (first page) results of USPTO Patent Page searches, which found:

- 135 issued patents with the word "useless" in the claims.
- 3 issued patents within class 713 (under which the '402 application is categorized) with the word "useless in the claims;
- 5 issued patents within class 380 (under which the '402 application was formerly categorized) with the word "useless in the claims;
- 547 issued patents within class 713 having the word "useless in the specification or the abstract, and
- 457 issued patents within class 380 having the word "useless in the specification or the abstract.

Atty. Docket No. 389522

Encryption literature likewise is rife with mentions of "useless" data, etc. For example, in laying out California's Data Breach Notification Act (SB 1386), "Legislators agreed that encryption provides a "safe harbor." In essence, they said that because *encrypted data is useless if obtained without authorization*, consumers would not be vulnerable to identify theft if a security breach occurred." "Data Encryption: The Foundation of Enterprise Security – Executive Summary," The Data Security Company, <http://americas.utimaco.com/encryption/Enterprise-security.html>, emphasis added.

In addition:

"Well-established computer *codes are rendered useless* if the user does not understand the underlying principles governing the code." Schwinkendorf, K.N., et al., "Pitfalls in computer code use in criticality analyses," Westinghouse Hanford Co., Richland, WA, Mar. 01, 1993, emphasis added. .

"Thus, the use of encryption *to render files useless* to anyone other than an authorized user is relevant both to files in transit and to those that reside on a server or a stand-alone computer". Cobb, Stephen, CISSP, "Encryption," Computer Security Handbook, 4th Edition, Wiley & Sons, 2002, p. T4-1, emphasis added. .

"An automated system that must overcome this Catch-22 must encrypt plaintext data in such a way that even the encrypting system itself is incapable of decrypting it. Asymmetric encryption algorithms provide a way to transform plaintext into ciphertext using *an encryption algorithm and a key that are useless for decryption.*" Coombs, Jason, "Programming Public Key CryptoStreams, Part I," Jan. 23, 2004, see <http://www.ddj.com/184416903>, emphasis added.

Given at least the evidence above, we submit that one skilled in the art would be able to understand "undecipherable" and "useless" in the context of the '402 Application. Thus, these terms are neither relative nor indefinite. We therefore respectfully request withdrawal of the Examiner's rejection.

#### 7. Claim Rejections – 35 U.S.C. § 112

Claims 15 and 16 stand rejected under 35 U.S.C. §112, the Examiner stating that "the term 'substantially' renders the claim an omnibus-type claim". Office Action, p. 3. Respectfully,

*Atty. Docket No. 389522*

the Examiner is wrong. MPEP is clear about the form of an omnibus claim, for example noting that "an omnibus claim... reads as follows: *A device substantially as shown and described.*" MPEP 2173.05(r), emphasis added.

Claim 15 does not recite "a device substantially as shown and described," instead reciting a secured computer network, comprising, among other elements, a host computer that executes an encrypted program using an encrypted data string, the host computer having substantially no intelligible or otherwise useful program code, computations or data associated with execution of the encrypted program.

Since claim 15 clearly does not match the MPEP example of an omnibus claim, and given the Examiner's reasoning (see above), we wonder if the Examiner believes that mere inclusion of the word "substantially" spawns an omnibus claim. However, this word does not in and of itself create an omnibus claim. Furthermore, the Federal Court has concluded that:

"the term 'substantially' is a descriptive term *commonly used in patent claims* to avoid a strict numerical boundary to the specified parameter...*when the term 'substantially' serves reasonably to describe the subject matter so that its scope would be understood by persons in the field of the invention, and to distinguish the claimed subject matter from the prior art, it is not indefinite*" Verve, LLC v. Crane Cams, Inc., No. 01-1417, Fed. Cir. Nov. 14, 2002, emphasis added.

Not surprisingly, the word "substantially" appears in tens of thousands of issued patents. A recent query on the USPTO Patent Search Page found over 86,000 patents with the word "substantially" in the claims. See Appendix C, attached.

Claim 15 is not an omnibus-type claim, and "substantially" is accepted and commonplace terminology. Thus, the remaining question is whether one of ordinary skill in the art would understand what is meant by a host computer having substantially no intelligible or otherwise useful program code, computations or data associated with execution of an encrypted program. We contend that the answer is yes. As noted above, there are a multitude of patents in the computer arts that include the words "useful" and/or "intelligible. One skilled in the art would understand "substantially no intelligible or otherwise useful program code, computations or data associated with execution of the encrypted program."

*Atty. Docket No. 389522*

However, in an effort to advance the '402 Application to issuance, claim 15 is amended to recite "...communicating results to the control computer for decoding, the host computer having insufficient intelligible program code, computations or data to execute the encrypted program." We submit that this language addresses the § 112 rejection. If the Examiner is not satisfied with these amendments to claim 15, we respectfully request that he suggest alternate claim language:

"Examiners are encouraged to suggest claim language to applicants to improve the clarity or precision of the language used, but should not reject claims or insist on their own preferences if other modes of expression selected by applicants satisfy the statutory requirement" MPEP 2173.02

Claim 16 depends from claim 15, and appears to be rejected under 35 U.S.C. §112 solely because of language in base claim 15. Thus, we believe that the amendment to claim 15 likewise addresses the rejection of claim 16. We respectfully request withdrawal of the Examiner's §112 rejection of both claims.

#### 8. Claim Rejections - 35 U.S.C. § 102

Claims 1-16 stand rejected as being anticipated by U.S. Patent No. 5,677,696 (hereinafter, "Silverstein"). We respectfully disagree.

Silverstein recites a method and apparatus for remotely calibrating a phased array antenna system, such as used in satellite communications systems. A phased array antenna consists of a number of elements that can radiate electromagnetic waveforms. Each element of the array delays and amplifies (or attenuates) a signal with respect to the other elements of the array so that the combined signal is steered towards a remote receiver. By analogy, consider two acoustic audio speakers, one closer to a listener than another. By appropriately delaying the signal that the closer speaker emits, the sound received by the listener can be either amplified or attenuated (even possibly cancelled).

Calibrating a phased array thus requires determining precise delays and gains (amplifications or attenuations) used by each radiating element with respect to a receiver. Because of physical variations in the array (such as variations in spatial positions due to flexibility of the array structure and variations in the digital logic of the delay and amplifier circuitry), the intended, programmed delay and gain settings can in fact differ from the delays

*Atty. Docket No. 389522*

and gains actually implemented by the array. In such cases, reference signals, known to both the transmitting array and receiving station, are sent so that the gains and delays can be easily estimated. Once the actual delays and gains are estimated by a specific ground station, the data sent by the satellite-based phased array can be processed to reconstruct the original signal with high fidelity and accuracy.

Accordingly, Silverstein's calibration method uses a specific combination of reference signals, based upon unitary transformations, so as to simplify the estimation of delay and gain settings of the array elements. Joint understanding of the specific calibration method by the transmitting array and a remote receiving station is fundamental to Silverstein. In other words, Silverstein's signals are not encrypted, and there is no encrypted execution by Silverstein's remote receiving station. Rather, Silverstein encodes signals and provides a remote station with decoding information (e.g., the inverse of the predetermined encoding matrix). The encoded signals and a reference signal are sent to the remote location, where the encoded signals are decoded and processed to generate calibration data for elements of the phased array system. In other words, contrary to Applicant's claims, Silverstein recites signals that are intelligible and useful to the remote location:

"upon performing suitable coherent detection *and decoding at the remote location*, the first and second sets of orthogonally encoded signals *allow for determining calibration data* indicative of any changes in the respective complex gains of the delay circuits, and including the respective signals {s(n) for n=1, 2, . . . , N} associated with each of the phased array elements". Silverstein col. 6, lines 6-12.

Moreover, the Silverstein patent is not concerned with the encrypted representation of computer programs or their execution on remote systems in encrypted form. The Silverstein patent does not mention general computer programs, their encryption or their execution on remote hosts.

#### Independent Claim 1

Turning now to the '402 claims, claim 1 clearly differs from (and is not anticipated by) Silverstein. Claim 1 recites a method for encrypting programs for encrypted execution on a computer network having a remote host computer. Silverstein nowhere mentions encrypting a

*Atty. Docket No. 389522*

program. Rather, as explained above, Silverstein encodes signals. A signal is not the same as a program. For this reason alone, Silverstein cannot anticipate claim 1.

However, claim 1 includes additional elements not taught or suggested by Silverstein. For example, contrary to the Examiner's statement, Silverstein does not encrypt a program as a unitary matrix with n rows and n columns. The Examiner points to Silverstein col. 4, lines 32-63 in support of this position. However, this passage describes encoding of a reference signal, not a computer program, using a unitary transformation and a technique for recovering the reference signal from such encoding. "Encoding," as used in Silverstein, is synonymous with representation, as in MP3 encoding of audio signals. This is different from encryption of programs, e.g., "in terms of random unitary matrix pre- and post-multiplications [that] results in Haar uniform probabilistic distribution of the encrypted programs--wherein any two programs or data strings of the same size that are encrypted separately according to this method will have the identical statistical distribution of all data in their encoded representations. Since all programs of a fixed size will have encrypted representations that are statistically indistinguishable, the remote computer will not be able to learn anything about a specific program because there is nothing that distinguishes any one such encrypted program from any other such encrypted program."

Specification p. 4, ¶3, line 3 of – p. 5, line 2

Next, Silverstein fails to teach or even suggest encrypting an input data string to a program, or executing a program on such an encrypted input data string. Contrary to the Examiner's assertion, Silverstein col. 9, line 51 – col. 10, line 49 does not teach this limitation. Rather, this passage presents a simple, concrete example of encoding a general signal into a calibrating reference signal by using a 4 by 4 Hadamard unitary matrix. It does not discuss (and Silverstein does not elsewhere discuss) encrypting data or computer programs, or the execution of encrypted computer programs on encrypted data strings. Rather, Silverstein sends encoded signals to a remote location, where they are decoded to allow for determining calibration data. See Silverstein col. 6, lines 6-12, quoted above. It does not appear that anything is done with the encoded signal at the remote location, before it is decoded. Decoding and using a signal is different from executing an encrypted program. For example, "In operation, a program to be executed on host 16 is first encrypted on control computer 12 and sent to host 16 over network 14... *Host 16 then executes an encrypted form of the program using the encrypted form of the data;* and transmits results through network 14. Control computer 12 (or another computer with

*Atty. Docket No. 389522*

the decode information) then accesses and decodes the results to determine the desired output." Specification p. 6, ¶2.

Also contrary to the Examiner's assertion, Silverstein col. 9, line 51 – col. 10, line 49 does not teach or suggest (a) loading an encrypted program and an encrypted data string on a host computer, (b) executing the encrypted program, using the encrypted data string, on the host computer, or (c) communicating results from the host computer to a network. Again, general computer programs are not discussed in Silverstein. Instead, Silverstein addresses the encoding and decoding of signals.

Further regarding element (a), Silverstein does not teach or suggest an encrypted program or an encrypted data string, and is thus also silent as loading such features on a host computer. Regarding element (b), it is critical to Silverstein that signal encodings are known to both the transmitting array and the receiving station. The form of Silverstein's encodings is completely transparent to all parties; thus, there is no execution or use of any "encrypted" element. Rather, Silverstein first decodes received signals, then processes the decoded signals to access calibration data.

Regarding element (c), not only does Silverstein fail to communicate results of encrypted execution (because there is no encrypted execution in Silverstein), but Silverstein also fails to make any mention of a network. Silverstein simply does not teach, suggest or depict a network. Rather, the cited passage (col. 9, line 51 – col. 10, line 49) addresses point to point communications systems such as a satellite and ground station.

Finally, Silverstein does not teach or suggest Applicant's final claim limitation – decoding results into output representative of executing a program with a data string, wherein computations and data associated with the program and data string are unintelligible and useless at the host computer. As noted above, Silverstein's remote location has decoding information, to decode received signals prior to processing to determine calibration data. Silverstein is specific and clear about the fact that the encoding must be known to both the transmitting array and receiver so that the calibration can be performed. Accordingly, and in contrast to claim 1, Silverstein does not disclose a technique wherein computations and data are unintelligible and useless at a host computer. Furthermore, claim 1 recites transmitting results to a network and

Atty. Docket No. 389522

then decoding results. Silverstein specifically teaches " decoding at the remote location," Silverstein col. 6, line 7.

Silverstein does not teach or suggest all of the limitations of claim 1; therefore, there is no anticipation. We respectfully request withdrawal of the Examiner's rejection, and allowance of claim 1.

**Dependent Claims 2-14**

These claims depend directly or indirectly from claim 1, and benefit from like argument. However, additional reasons for patentability of claims 2-14 include the following:

Claim 2 recites converting a program to a unitary matrix multiplication. Silverstein does not teach or suggest this feature. Instead, at the passage cited by the Examiner and elsewhere, Silverstein presents an example encoding of a known signal by a known unitary matrix transformation without any reference to encryption of programs or data. The signal and transformation is known to all parties for the purpose of calibration.

Claim 3 depends from claim 2 and benefits from like argument. Claim 3 also recites converting a program to a unitary matrix multiplication  $U$  such that  $U \in U_n$  for some integer  $n$ , where  $U_n$  represents a group of unitary matrices of size  $n$ . Silverstein does not teach or suggest this limitation. For example, at cited col. 4, lines 32-63, Silverstein discusses using standard unitary transformations such Hadamard or Fourier transformations which are known to both the transmitter and receiver. This is different from converting a program to a unitary matrix multiplication.

Claim 4 depends from claim 3, and benefits from like argument. Further, claim 4 recites generating two independent identically distributed unitary matrices  $X, Y$  from a uniform probability distribution over  $U_n$  determined by the Haar distribution. Silverstein is silent as to the Haar distribution, and does not mention, reference or even hint at generating independent unitary matrices from the Haar distribution. Likewise, Silverstein is mum as to encrypting a program using such matrices.

Claim 5 depends from claim 4, thus benefiting from like argument. In addition, claim 5 recites the unique element of computing  $U'$  as  $XUY^*$  and communicating  $U'$  to the remote host computer over the network. Silverstein does not, at the Examiner's cited passage or elsewhere, mention, reference or suggest computing a product of three unitary matrices, two being the

*Atty. Docket No. 389522*

randomly generated unitary matrices and the third being the computer program represented as a unitary matrix. See claims 2-4, above.

Claim 6 also depends from claim 4, and benefits from like argument. Claim 6 also recites converting the input data string to a vector b. Silverstein col. 8, lines 9-46 does not teach or suggest converting an input data string to a computer program into a vector. Rather, the referenced section of Silverstein discusses the representation of a signal using complex phasor representations which are standard technique for signal representation and are not encrypted in any way. Silverstein fails to teach or suggest the limitations of claim 6, anywhere.

Claim 7 depends from claim 6, and further recites computing b' as Yb and communicating b' to the remote host over the network. Silverstein does not teach or suggest this element. The passage (col. 8, lines 9-46) cited by the Examiner recites representation of a known signal transmitted by a phased array. This is different from computing a product of a (converted input data string) vector and a unitary matrix. See claims 4-6, above.

Claim 8 depends from claims 6 and 7, and benefits from like argument. Claim 8 also recites computing the product of XUY\* and Yb and communicating results to the network. The passage cited by the Examiner does not teach or suggest this limitation. Rather, col. 9, lines 24-46 describes operations of the remote receiving ground station that are required to estimate the calibration information. All the transformations used are known to both the transmitting array and receiving station so that there is no encryption of data or programs whatsoever. As noted, Silverstein also fails to teach or suggest a network.

Claim 9 depends from claim 8, and benefits from like argument. In addition, claim 9 recites decoding comprising computing X\*XUb, external of the host computer, to determine the multiplication of Ub as desired output of the program, wherein XUY\* and Yb is (XUb) and X\*XUb is obtained by matrix multiplication X\*(XUb). The Examiner uses the same passage in an attempt to show the limitations of claim 9 within Silverstein. However, this passage addresses the decoding of a received signal by Silverstein's ground station; using the known (not encrypted) transformation. Silverstein encodes a signal (indicative of calibrations performed) at the array and decodes the signal at the receiving ground station. Here, Silverstein's remote host performs an operation and then encodes information representative of the operation. This is different from the inventions of the '402 Application, where computations and data are hidden

*Atty. Docket No. 389522*

from the remote host on which execution is performed. Silverstein does not involve encryption and does not involves hiding data or computations. On the contrary, all information in Silverstein is know to all participating entities.

Claim 10 recites decrypting at a control computer connected to the network and the host computer. Since Silverstein does not address encrypting at all, Silverstein also does not teach or suggest decrypting, let alone decrypting of information representative of results of executing an encrypted program.

Claims 11-13 recite the Internet, a virtual private network and a local area network (LAN), respectively. Silverstein does not, at the referenced col. 3, lines 27-42 or elsewhere, teach or suggest any such features. Instead, this passage explicitly describes radio frequency (RF) communication from a satellite to a ground station. The terms "Internet," "Network," "LAN," "local area," "private" and "virtual" are completely absent from Silverstein.

Claim 14 recites embedding one or more constants into the input data string or program, prior to encrypting, to detect incorrect execution or data tampering. The Examiner states that such features are disclosed at Silverstein col. 16, line 1 – col. 17, line 67. However, the Silverstein patent ends at column 12. We thus respectfully request the Examiner's clarification; however, we contend that nowhere does Silverstein teach or suggest the elements of claim 14. For example, as noted above, Silverstein does not encrypt an input data string or a program. Furthermore, the only constants mentioned in Silverstein are propagation constants. Silverstein does not indicate that these propagation constants are used to detect incorrect execution or data tampering.

Claims 2-14 are clearly not anticipated by Silverstein. We therefore respectfully request withdrawal of the Examiner's rejection, and allowance of each of these dependent claims.

#### Independent Claim 15

Claim 15 likewise stands rejected as being anticipated by Silverstein. However, claim 15 recites a secured computer network for executing encrypted computer programs at a remote host computer, without sharing intelligible or otherwise useful program code, computations or data associated with execution. Respectfully, as noted above, Silverstein does not address computer networks, encrypted programs or encrypted execution. In fact, Silverstein recites open communication where a remote location has the necessary information to decode signals that are

*Atty. Docket No. 389522*

received from a ground station. The signals are decoded by the remote location, to determine calibration information. In other words, Silverstein's method and apparatus requires that the remote location and the ground location share data associated with received signals. See arguments in support of claim 1, above.

In addition, claim 15 recites a control computer for encrypting a program as a unitary matrix and for encrypting an input data string to the program, as a vector. Silverstein teaches no such thing. Again, Silverstein does not encrypt programs, at all.

Claim 15 also recites execution of the program on the input data string, by matrix multiplication of the unitary matrix with the vector. Silverstein fails to teach or suggest this claim element.

Next, claim 15 recites a host computer, *in network with* the control computer. Silverstein does not teach or suggest a computer network. Silverstein is likewise mum as to the claim 15 elements of loading an encrypted program and an encrypted data string.

Silverstein also fails to teach or suggest a host computer executing an encrypted program, using an encrypted data string, and communicating results to the control computer for decoding. Rather, Silverstein receives encoded signals at a remote location and decodes the signals to determine calibration information for a phased array. See Silverstein col. 6, lines 6-12.

Finally, Silverstein does not teach or suggest a host computer having insufficient intelligible program code, computations or data to execute the encrypted program. On the contrary, Silverstein requires that the remote location be able to decode received signals, in order to use the signals for calibration purposes.

As shown, Silverstein does not teach or suggest every claim element, and therefore cannot anticipate claim 15. Withdrawal of the Examiner's rejection, and allowance of claim 15, are thus respectfully requested.

#### Dependent claim 16

Claim 16 depends from claim 15 and is thus believed allowable for at least this reason. However claim 16 also recites a control computer that embeds one or more constants into the unitary matrix or data string, wherein the results from the host computer indicate tampering or incorrect execution of the encrypted program. Silverstein plainly does not teach or suggest this

*Atty. Docket No. 389522*

element. See, e.g., arguments in support of claim 14, above. We thus respectfully request withdrawal of the Examiner's rejection, and allowance of claim 16.

#### CONCLUSION

In view of the above clarifying Amendments and Remarks, Applicant respectfully solicits a Notice of Allowance for all of pending claims 1-16. Should any issues remain outstanding, we encourage the Examiner to telephone Applicant's attorney, Curtis A. Vock, at (720) 931-3011, prior to issuing any further Office Communication.

This Amendment and Response is submitted with a Petition for One Month's Extension of Time, along with authorization to charge the required extension fee to Deposit Account No. 12-0600. No other fees are believed due; however, if any additional fee is deemed necessary in connection with this Amendment and Response, please charge Deposit Account No. 12-0600.

Respectfully submitted,

LATHROP & GAGE L.C.

Date: 19 Feb. 2007

By: Heather F. Perrin

Heather F. Perrin, Reg. No. 52,884  
4845 Pearl East Circle, Suite 300  
Boulder, Colorado 80301  
Tele: (720) 931-3033  
Fax: (720) 931-3001

## Patent Database Search Results: ACLM/unintelligible in US Patent Collection

Page 1 of 2

USPTO PATENT FULL-TEXT AND IMAGE DATABASE

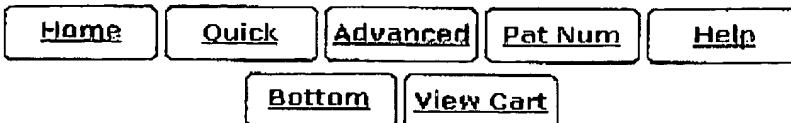
Home	Quick	Advanced	Pat Num	Help
Next List	Bottom	View Cart		

*Searching US Patent Collection...***Results of Search in US Patent Collection db for:****ACLM/unintelligible: 79 patents.****Hits 1 through 50 out of 79****[Next 50 Hits]****[Jump To] [ ]****[Refine Search] [ACLM/unintelligible]**PAT.      Title  
NO.

- 1 7,143,028 T Method and system for masking speech
- 2 6,985,869 T Digital prescription carrier and monitor system
- 3 6,935,943 T Wireless communication for fume hood control
- 4 6,927,779 T Web-based well plate information retrieval and display system
- 5 6,868,159 T 'Virtual' encryption scheme combining different encryption operators into compound-encryption mechanism
- 6 6,834,312 T Method and apparatus for delivery of data over a network
- 7 6,779,747 T Intelligent document shredder device
- 8 6,477,492 T System for automated testing of perceptual distortion of prompts from voice response systems
- 9 6,243,465 T Method of providing video programming nearly on demand
- 10 6,233,338 T Virtual encryption scheme combining different encryption operators into compound-encryption mechanism
- 11 6,215,982 T Wireless communication method and device with auxiliary receiver for selecting different channels
- 12 6,189,446 T System for the secure destruction of compact disc data
- 13 6,137,884 T Simultaneous electronic transactions with visible trusted parties
- 14 6,134,326 T Simultaneous electronic transactions
- 15 6,097,812 T Cryptographic system
- 16 5,995,638 T Methods and apparatus for authentication of documents by using the intensity profile of moire patterns
- 17 5,980,385 T Electronic apparatus and method of assisting in the play of a game and tickets used therewith
- 18 5,974,548 T Media-independent document security method and apparatus
- 19 5,929,801 T Method for repeating interrogations until failing to receive unintelligible responses to identify plurality of transponders by an interrogator

Patent Database Search Results: CCL/380/\$ AND ACLM/unintelligible in US Patent Collection

Page 1 of 2

**USPTO PATENT FULL-TEXT AND IMAGE DATABASE***Searching US Patent Collection...*

**Results of Search in US Patent Collection db for:**  
**(CCL/380/\$ AND ACLM/unintelligible): 30 patents.**  
*Hits 1 through 30 out of 30*

 [ ] [CCL/713/\$ AND ACLM/unintelligible]

PAT. NO. Title

1. 7,143,028 T Method and system for masking speech
2. 6,868,159 T 'Virtual' encryption scheme combining different encryption operators into compound-encryption mechanism
3. 6,243,465 T Method of providing video programming nearly on demand
4. 6,233,338 T Virtual encryption scheme combining different encryption operators into compound-encryption mechanism
5. 6,137,884 T Simultaneous electronic transactions with visible trusted parties
6. 6,134,326 T Simultaneous electronic transactions
7. 6,097,812 T Cryptographic system
8. 5,995,638 T Methods and apparatus for authentication of documents by using the intensity profile of moire patterns
9. 5,974,548 T Media-independent document security method and apparatus
10. 5,629,982 T Simultaneous electronic transactions with visible trusted parties
11. 5,583,937 T Method for providing video programming nearly on demand
12. 5,307,410 T Interferometric quantum cryptographic key distribution system
13. 5,199,067 T Process for promotion of pay television broadcasts, and device for use of the process
14. 5,181,243 T System and method for communications security protection
15. 5,148,478 T System and method for communications security protection
16. 5,054,064 T Video control system for recorded programs
17. 5,046,092 T Video control system for transmitted programs
18. 5,046,090 T Recorded medium for video control system
19. 4,991,208 T Video control system having session encryption key
20. 4,731,839 T Method for coding and de-coding audio and video information
21. 4,682,224 T System, method, and apparatus for television signal scrambling and descrambling
22. 4,573,205 T Technique for secure communications on FM radio channels

Patent Database Search Results: CCL/713/\$ AND ACLM/intelligible in US Patent Collection

Page 1 of 1

**USPTO PATENT FULL-TEXT AND IMAGE DATABASE**[Home](#)[Quick](#)[Advanced](#)[Pat Num](#)[Help](#)[Bottom](#)[View Cart](#)*Searching US Patent Collection...***Results of Search in US Patent Collection db for:****(CCL/713/\$ AND ACLM/intelligible): 13 patents.***Hits 1 through 13 out of 13*[Jump To:](#) [Refine Search](#)

CCL/380/\$ AND ACLM/unintelligible

PAT. NO. Title

- 1 [6,959,090 T Content Protection scheme for a digital recording device](#)
- 2 [6,957,199 T Method, system and service for conducting authenticated business transactions](#)
- 3 [6,917,724 T Methods for opening file on computer via optical sensing](#)
- 4 [6,745,326 T Authentication process including setting up a secure channel between a subscriber and a service provider accessible through a telecommunications operator](#)
- 5 [6,408,389 T System for supporting secured log-in of multiple users into a plurality of computers using combined presentation of memorized password and transportable passport record](#)
- 6 [6,339,828 T System for supporting secured log-in of multiple users into a plurality of computers using combined presentation of memorized password and transportable passport record](#)
- 7 [6,137,884 T Simultaneous electronic transactions with visible trusted parties](#)
- 8 [6,081,893 T System for supporting secured log-in of multiple users into a plurality of computers using combined presentation of memorized password and transportable passport record](#)
- 9 [5,953,419 T Cryptographic file labeling system for supporting secured access by multiple users](#)
- 10 [5,748,895 T System for remotely programming a portable information device using visible optical pattern transmitted from a display device while concurrently displaying human-readable explanation of the pattern](#)
- 11 [5,553,145 T Simultaneous electronic transactions with visible trusted parties](#)
- 12 [5,181,243 T System and method for communications security protection](#)
- 13 [5,168,519 T System and method for securing DTMF transmission](#)

[Top](#)[View Cart](#)[Home](#)[Quick](#)[Advanced](#)[Pat Num](#)[Help](#)

Patent Database Search Results: ((ccl/713/\$) and ((spec/unintelligible) or (abst/unintelligible))) in... Page 1 of 2

## USPTO PATENT FULL-TEXT AND IMAGE DATABASE

Home	Quick	Advanced	Pat Num	Help
Next List	Bottom	View Cart		

Searching US Patent Collection...

Results of Search in US Patent Collection db for:  
(CCL/713/\$ AND (SPEC/unintelligible OR ABST/unintelligible)): 195 patents.  
Hits 1 through 50 out of 195

[Next 50 Hits](#)

[Jump To:](#)

[Refine Search](#) | ((ccl/713/\$) and ((spec/unintelligible) or (abst/unintelligible)))

PAT.	NO.	Title
1	<a href="#">7,165,180</a>	<a href="#">T Monolithic semiconductor device for preventing external access to an encryption key</a>
2	<a href="#">7,146,495</a>	<a href="#">T Digital document storage</a>
3	<a href="#">7,137,008</a>	<a href="#">T Flexible method of user authentication</a>
4	<a href="#">7,130,368</a>	<a href="#">T Clock recovery using a direct smoothing process</a>
5	<a href="#">7,124,305</a>	<a href="#">T Data repository and method for promoting network storage of data</a>
6	<a href="#">7,120,696</a>	<a href="#">T Cryptographic communications using pseudo-randomly generated cryptography keys</a>
7	<a href="#">7,120,253</a>	<a href="#">T Method and system for protecting video data</a>
8	<a href="#">7,116,781</a>	<a href="#">T Counteracting geometric distortions in watermarking</a>
9	<a href="#">7,113,593</a>	<a href="#">T Recursive cryptoaccelerator and recursive VHDL design of logic circuits</a>
10	<a href="#">7,082,199</a>	<a href="#">T Simple encrypted transmission system suitable for intermittent signals</a>
11	<a href="#">7,076,661</a>	<a href="#">T System for denying access to content generated by a compromised off line encryption device and for conveying cryptographic keys from multiple conditional access systems</a>
12	<a href="#">7,073,055</a>	<a href="#">T System and method for providing distributed and dynamic network services for remote access server users</a>
13	<a href="#">7,072,490</a>	<a href="#">T Symmetry watermark</a>
14	<a href="#">7,069,437</a>	<a href="#">T Multi-level security network system</a>
15	<a href="#">7,039,807</a>	<a href="#">T Method and system for obtaining digital signatures</a>
16	<a href="#">7,024,558</a>	<a href="#">T Apparatus and method for authenticating digital signatures and computer-readable recording medium thereof</a>
17	<a href="#">7,020,791</a>	<a href="#">T Clock recovery using a double-exponential smoothing process</a>
18	<a href="#">7,020,776</a>	<a href="#">T Cryptosystem based on a Jacobian of a curve</a>
19	<a href="#">7,010,685</a>	<a href="#">T Method and apparatus for storing scrambled digital programs by filtering product identifier</a>
20	<a href="#">7,003,667</a>	<a href="#">T Targeted secure printing</a>

Patent Database Search Results: ((ccl/380\$) and ((spec/unintelligible) or (abst/unintelligible))) in ... Page 1 of 2

## USPTO PATENT FULL-TEXT AND IMAGE DATABASE

Home	Quick	Advanced	Pat. Num.	Help
Next List	Bottom	View Cart		

*Searching US Patent Collection...*

**Results of Search in US Patent Collection db for:**  
**(CCL/380\$ AND (SPEC/unintelligible OR ABST/unintelligible)): 431 patents.**  
*Hits 1 through 50 out of 431*

((ccl/380\$) and ((spec/unintelligible) or (abst/unintelligible)))

PAT.	NO.	Title
1	7,165,180	T <u>Monolithic semiconductor device for preventing external access to an encryption key</u>
2	7,158,640	T <u>Method and apparatus for re-synchronization of a stream cipher during handoff</u>
3	7,151,832	T <u>Dynamic encryption and decryption of a stream of data</u>
4	7,149,309	T <u>Time-dependent authorization</u>
5	7,149,308	T <u>Cryptographic communications using in situ generated cryptographic keys for conditional access</u>
6	7,143,028	T <u>Method and system for masking speech</u>
7	7,142,672	T <u>Method and system for transmitting sensitive information over a network</u>
8	7,133,522	T <u>Method and apparatus for encryption of data</u>
9	7,120,696	T <u>Cryptographic communications using pseudo-randomly generated cryptography keys</u>
10	7,120,253	T <u>Method and system for protecting video data</u>
11	7,116,781	T <u>Counteracting geometric distortions in watermarking</u>
12	7,113,596	T <u>Embedding information related to a subject of an identification document in the identification document</u>
13	7,113,593	T <u>Recursive cryptoaccelerator and recursive VHDL design of logic circuits</u>
14	7,082,199	T <u>Simple encrypted transmission system suitable for intermittent signals</u>
15	7,080,397	T <u>Communication protocol for content on demand system with callback time</u>
16	7,079,651	T <u>Cryptographic method and apparatus for non-linearly merging a data block and a key</u>
17	7,076,661	T <u>System for denying access to content generated by a compromised off line encryption device and for conveying cryptographic keys from multiple conditional access systems</u>
18	7,072,490	T <u>Symmetry watermark</u>
19	7,065,210	T <u>Secret key generation method, encryption method, cryptographic communications method, common key generator, cryptographic communications system, and recording media</u>

T

## Patent Database Search Results: ACLM/useless in US Patent Collection

Page 1 of 2

**USPTO PATENT FULL-TEXT AND IMAGE DATABASE**

<a href="#">Home</a>	<a href="#">Quick</a>	<a href="#">Advanced</a>	<a href="#">Pat Num</a>	<a href="#">Help</a>
<a href="#">Next List</a>	<a href="#">Bottom</a>	<a href="#">View Cart</a>		

*Searching US Patent Collection...***Results of Search in US Patent Collection db for:****ACLM/useless: 135 patents.***Hits 1 through 50 out of 135*[Next 50 Hits](#)[Jump To](#)[Refine Search](#)

ACLM/useless

PAT.  
NO.

	PAT. NO.	Title
1	<a href="#">7,153,116</a>	<a href="#">T Resin molding machine</a>
2	<a href="#">7,139,597</a>	<a href="#">T Living body light measuring device</a>
3	<a href="#">7,079,690</a>	<a href="#">T Method and apparatus for editing an image while maintaining codestream size</a>
4	<a href="#">7,073,739</a>	<a href="#">T Crushing-breaking method of casting products, cutter structure used for the method and crushing-breaking apparatus of casting products</a>
5	<a href="#">7,054,856</a>	<a href="#">T System for drawing patent map using technical field word and method therefor</a>
6	<a href="#">7,050,439</a>	<a href="#">T Method for performing discontinuous transmission in an asynchronous transfer mode</a>
7	<a href="#">7,042,659</a>	<a href="#">T Optical lens, design method for the optical lens and lens system using the optical lens</a>
8	<a href="#">7,037,628</a>	<a href="#">T Method of a floating pattern loading system in mask dry-etching critical dimension control</a>
9	<a href="#">7,010,125</a>	<a href="#">T Method for tracing traitor receivers in a broadcast encryption system</a>
10	<a href="#">6,931,631</a>	<a href="#">T Low impact breakpoint for multi-user debugging</a>
11	<a href="#">6,925,562</a>	<a href="#">T Scheme for blocking the use of lost or stolen network-connectable computer systems</a>
12	<a href="#">6,911,729</a>	<a href="#">T Tape carrier semiconductor device</a>
13	<a href="#">6,886,085</a>	<a href="#">T Method and apparatus for efficient virtual memory management</a>
14	<a href="#">6,871,019</a>	<a href="#">T Shutter abnormality detection apparatus for camera</a>
15	<a href="#">6,869,816</a>	<a href="#">T Deposition method for balancing film stress</a>
16	<a href="#">6,857,060</a>	<a href="#">T System, apparatus and method for prioritizing instructions and eliminating useless instructions</a>
17	<a href="#">6,845,061</a>	<a href="#">T Method for quickly detecting the state of a nonvolatile storage medium</a>
18	<a href="#">6,832,914</a>	<a href="#">T Preform allowing the production of personalized orthodontic apparatuses following deformation, the apparatuses obtained and the process for their production</a>
19	<a href="#">6,832,058</a>	<a href="#">T Image forming apparatus including a maximum charge quantity of toner particles forming useless toner</a>
20	<a href="#">6,801,638</a>	<a href="#">T Device and method for recognizing traffic signs</a>

Patent Database Search Results: ((ccl/713/\$) and (aclm/useless)) in US Patent Collection

Page 1 of 1

**USPTO PATENT FULL-TEXT AND IMAGE DATABASE**

<a href="#">Home</a>	<a href="#">Quick</a>	<a href="#">Advanced</a>	<a href="#">Pat Num</a>	<a href="#">Help</a>
<a href="#">Bottom</a>	<a href="#">View Cart</a>			

*Searching US Patent Collection...***Results of Search in US Patent Collection db for:****(CCL/713/\$ AND ACLM/useless): 3 patents.***Hits 1 through 3 out of 3*[Jump To:](#) [Refine Search](#) | ((ccl/713/\$) and (aclm/useless))

PAT. NO. Title

- 1 [6,925,562](#) T [Scheme for blocking the use of lost or stolen network-connectable computer systems](#)
- 2 [6,550,010](#) T [Method and apparatus for a unit locked against use until unlocked and/or activated on a selected network](#)
- 3 [6,018,712](#) T [Method and apparatus for remote program execution to use in computer software protection without the use of encryption](#)

<a href="#">Home</a>	<a href="#">Quick</a>	<a href="#">Advanced</a>	<a href="#">Pat Num</a>	<a href="#">Help</a>
<a href="#">Top</a>	<a href="#">View Cart</a>			

Patent Database Search Results: ((ccl/380/\$) and (aclm/useless)) in US Patent Collection

Page 1 of 1

**USPTO PATENT FULL-TEXT AND IMAGE DATABASE**

<a href="#">Home</a>	<a href="#">Quick</a>	<a href="#">Advanced</a>	<a href="#">Pat Num</a>	<a href="#">Help</a>
<a href="#">Bottom</a>	<a href="#">View Cart</a>			

*Searching US Patent Collection...***Results of Search in US Patent Collection db for:****(CCL/380/\$ AND ACLM/useless): 5 patents.***Hits 1 through 5 out of 5*

<a href="#">Jump To</a>	<input type="text"/>
-------------------------	----------------------

<a href="#">Refine Search</a>	((ccl/380/\$) and (aclm/useless))
-------------------------------	-----------------------------------

PAT. NO. Title

- 1 [7,010,125](#) T [Method for tracing traitor receivers in a broadcast encryption system](#)
- 2 [6,925,562](#) T [Scheme for blocking the use of lost or stolen network-connectable computer systems](#)
- 3 [5,519,778](#) T [Method for enabling users of a cryptosystem to generate and use a private pair key for enciphering communications between the users](#)
- 4 [4,736,422](#) T [Encrypted broadcast television system](#)
- 5 [4,663,664](#) T [Electronic ticket method and apparatus for television signal scrambling and descrambling](#)

<a href="#">Top</a>	<a href="#">View Cart</a>			
<a href="#">Home</a>	<a href="#">Quick</a>	<a href="#">Advanced</a>	<a href="#">Pat Num</a>	<a href="#">Help</a>

Patent Database Search Results: ((ccl/713/\$) and ((spec/useless) or (abst/useless))) in US Patent ... Page 1 of 2

**USPTO PATENT FULL-TEXT AND IMAGE DATABASE**

<a href="#">Home</a>	<a href="#">Quick</a>	<a href="#">Advanced</a>	<a href="#">Pat Num</a>	<a href="#">Help</a>
<a href="#">Next List</a>	<a href="#">Bottom</a>	<a href="#">View Cart</a>		

Searching US Patent Collection...

**Results of Search in US Patent Collection db for:**  
**(CCL/713/\$ AND (SPEC/useless OR ABST/useless)): 547 patents.**  
Hits 1 through 50 out of 547

[Next 50 Hits](#)[Jump To](#) [Refine Search](#) | ((ccl/713/\$) and ((spec/useless) or (abst/useless)))PAT.  
NO. Title

- 1 [7,165,180 T Monolithic semiconductor device for preventing external access to an encryption key](#)
- 2 [7,165,175 T Apparatus, system and method for selectively encrypting different portions of data sent over a network](#)
- 3 [7,165,174 T Trusted infrastructure support systems, methods and techniques for secure electronic commerce transaction and rights management](#)
- 4 [7,158,954 T System and method for processing protected video information](#)
- 5 [7,155,608 T Foreign network SPAM blocker](#)
- 6 [7,155,035 T Personal authentication method, personal authentication apparatus and image capturing device](#)
- 7 [7,149,895 T Personal device, terminal, server and methods for establishing a trustworthy connection between a user and a terminal](#)
- 8 [7,149,823 T System and method for direct memory access from host without processor intervention wherein automatic access to memory during host start up does not occur](#)
- 9 [7,149,311 T Methods and apparatus for providing networked cryptographic devices resilient to capture](#)
- 10 [7,149,310 T Method and system for authorizing generation of asymmetric crypto-keys](#)
- 11 [7,146,644 T Data security system and method responsive to electronic attacks](#)
- 12 [7,146,495 T Digital document storage](#)
- 13 [7,143,440 T User authentication system and method](#)
- 14 [7,143,295 T Methods and circuits for dedicating a programmable logic device for use with specific designs](#)
- 15 [7,143,294 T Apparatus and method for secure field upgradability with unpredictable ciphertext](#)
- 16 [7,143,287 T Method and system for verifying binding of an initial trusted device to a secured processing system](#)
- 17 [7,140,044 T Data security system and method for separation of user communities](#)
- 18 [7,139,914 T System and method for network security](#)
- 19 [7,139,737 T Apparatus and method for managing software licenses and storage medium storing a program](#)

Patent Database Search Results: ((ccl/380/\$) and ((spec/useless) or (abst/useless))) in US Patent ... Page 1 of 2

**USPTO PATENT FULL-TEXT AND IMAGE DATABASE**

<a href="#">Home</a>	<a href="#">Quick</a>	<a href="#">Advanced</a>	<a href="#">Pat Num</a>	<a href="#">Help</a>
<a href="#">Next List</a>	<a href="#">Bottom</a>	<a href="#">View Cart</a>		

*Searching US Patent Collection...*

**Results of Search in US Patent Collection db for:**  
**(CCL/380/\$ AND (SPEC/useless OR ABST/useless)): 457 patents.**  
*Hits 1 through 50 out of 457*

[Next 50 Hits](#)[Jump To](#) [Refine Search](#)  ((ccl/380/\$) and ((spec/useless) or (abst/useless)))PAT.  
NO.

	PAT. NO.	Title
1	<a href="#">7,165,180</a>	<a href="#">T Monolithic semiconductor device for preventing external access to an encryption key</a>
2	<a href="#">7,158,954</a>	<a href="#">T System and method for processing protected video information</a>
3	<a href="#">7,158,800</a>	<a href="#">T Method and system for limiting content diffusion to local receivers</a>
4	<a href="#">7,149,895</a>	<a href="#">T Personal device, terminal, server and methods for establishing a trustworthy connection between a user and a terminal</a>
5	<a href="#">7,149,311</a>	<a href="#">T Methods and apparatus for providing networked cryptographic devices resilient to capture</a>
6	<a href="#">7,149,310</a>	<a href="#">T Method and system for authorizing generation of asymmetric crypto-keys</a>
7	<a href="#">7,143,440</a>	<a href="#">T User authentication system and method</a>
8	<a href="#">7,139,737</a>	<a href="#">T Apparatus and method for managing software licenses and storage medium storing a program for managing software licenses</a>
9	<a href="#">7,131,004</a>	<a href="#">T Method and apparatus for encrypting data transmitted over a serial link</a>
10	<a href="#">7,130,425</a>	<a href="#">T Method and apparatus for providing a bus-encrypted copy protection key to an unsecured bus</a>
11	<a href="#">7,124,302</a>	<a href="#">T Systems and methods for secure transaction management and electronic rights protection</a>
12	<a href="#">7,120,421</a>	<a href="#">T Wireless network with a cipher key change procedure</a>
13	<a href="#">7,120,249</a>	<a href="#">T Methods and systems for generating encryption keys using random bit generators</a>
14	<a href="#">7,116,781</a>	<a href="#">T Counteracting geometric distortions in watermarking</a>
15	<a href="#">7,114,047</a>	<a href="#">T Data storage medium with certification data</a>
16	<a href="#">7,113,596</a>	<a href="#">T Embedding information related to a subject of an identification document in the identification document</a>
17	<a href="#">7,113,595</a>	<a href="#">T Generation of a random number that is non-divisible by a set of prime numbers</a>
18	<a href="#">7,111,173</a>	<a href="#">T Encryption process including a biometric unit</a>
19	<a href="#">7,111,165</a>	<a href="#">T Key and lock device</a>
20	<a href="#">7,107,616</a>	<a href="#">T Method of producing a response</a>

## Patent Database Search Results: ACLM/substantially in US Patent Collection

Page 1 of 2

**USPTO PATENT FULL-TEXT AND IMAGE DATABASE**

<a href="#">Home</a>	<a href="#">Quick</a>	<a href="#">Advanced</a>	<a href="#">Pat Num</a>	<a href="#">Help</a>
<a href="#">Next List</a>	<a href="#">Bottom</a>	<a href="#">View Cart</a>		

*Searching US Patent Collection...***Results of Search in US Patent Collection db for:****ACLM/substantially: 860210 patents.***Hits 1 through 50 out of 860210*[Next 50 Hits](#)[Jump To](#)[Refine Search](#) | **ACLM/substantially**

PAT.  
NO.      Title

- 1 [RE39,472 T Golf putter having improved marking](#)
- 2 [RE39,469 T Semiconductor integrated circuit with mixed gate array and standard cell](#)
- 3 [RE39,465 T Modular sleeve yoke](#)
- 4 [PP17,359 T Miniature rose plant named 'Poulpah035'](#)
- 5 [PP17,358 T Black walnut tree named 'Beineke 14'](#)
- 6 [PP17,357 T Portulaca plant named 'Balrioscar'](#)
- 7 [PP17,356 T Buffalograss plant named 'Density'](#)
- 8 [PP17,355 T Antirrhinum plant named 'Balumsum'](#)
- 9 [D535,442 T Cosmetic compact](#)
- 10 [D535,313 T Tire changer jaw](#)
- 11 [D535,308 T Media device](#)
- 12 [D535,286 T Communication headset](#)
- 13 [D535,207 T Face display for a timepiece](#)
- 14 [D535,206 T Face display for a timepiece](#)
- 15 [D535,171 T Knife](#)
- 16 [D535,111 T Flexible apparel hook](#)
- 17 [7,165,233 T Test ket layout for precisely monitoring 3-sail lens aberration effects](#)
- 18 [7,165,206 T SRAM-compatible memory for correcting invalid output data using parity and method of driving the same](#)
- 19 [7,165,205 T Method and apparatus for encoding and decoding data](#)
- 20 [7,165,191 T Automated verification of user interface tests on low-end emulators and devices](#)
- 21 [7,165,184 T Transferring data between differently clocked busses](#)
- 22 [7,165,127 T Flow control for interfaces providing retransmission](#)